

Patent Application for:

Authenticating Digital Records

Inventor: Jaffer Qamar
A citizen of the United States of America
Residing at:
98 Cervantes Blvd., #1
San Francisco, CA 94123

CERTIFICATE OF EXPRESS MAIL

I hereby certify that this paper and all enclosures are being deposited in a single envelope with the United States Postal Service as "Express Mail Post Office Addressee" Service under 37 CFR §1.10 on 02/09/04, having "Express Mail" label No.: ER 394053745 US,

addressed to: Mail Stop Patent Application, Commissioner for Patents, P.O. Box 1450 Arlington, VA 22313-1450.

Signature of Person Mailing Correspondence: Jaffer Qamar

Printed Name: Jaffer Qamar

SPECIFICATION**Authenticating Digital Records****BACKGROUND OF THE INVENTION**

- [0001] Many people are forced to rely on the representations of others (individuals or organizations) with regards to information about themselves, items they wish to sell, pets they wish to sell or give away, children they wish to put up for adoption, services they wish to provide, events that have occurred, places to visit, properties for sale, documents (including drawings, tickets and legal claims) in their possession, sound or video recordings, artwork, plants, or claims about how certain devices or processes work. Many people forgo transaction opportunities or relationships because of potential for and risk of misrepresentation and fraud.
- [0002] Such fraud has traditionally been mitigated in paper transactions by the use of notary services and secure access to information. That is, generally speaking, people have created and compiled records and then signed them, either under penalty of perjury, or before a notary public. The notary verifies the signature and the signer's identity and certifies with a seal, its name and signature, the date and place of certification, to assure a third party (the recipient of the record) that the signer is the person who he claims to be. The notary does not authenticate the record attributes (or its contents), which is the duty of the signer. To avoid misrepresentation, the certifying authority should add record attributes and the identifying information of the record provider (record supplier). Such information, which is accurate, recent and reliable, protects recipients.
- [0003] Organizations transacting (dealing) with customers (audience) try to mitigate misrepresentation by building reputations. But, sometimes, even they misrepresent, under stress or when their representative tries to benefit himself rather than promote the organization.
- [0004] Known methods for authenticating are: (1) Verifying an individual's identity before permitting him access to secure information, a secure server (for example, for voting), or to a secure location. (2) Computer-created files having date and

time stamps that show when the records were created. (3) A service-provider verifying the identity of an entity by checking public records and certifying the entity with its seal and a date stamp. (4) A notary public certifying the signature and the identity of the person signing a record by attesting its seal, signature, date and location. (5) A computer-based system verifying a person's signature by digitally matching it with the one on its server and, if needed, extending the certification period.

- [0005] Some prior art includes a review or a story covered in a magazine, newspaper, TV report, consumer report, or a government agency that investigates people, events, incidents, places, objects, products, services, advertisements, claims and commitments made by my organizations or individuals to customers or their constituents. Determinations made by an independent entity, however, are not initiated by the record-owner (record-provider) and, when they are, the final record (including the determinations made by the independent entity) is not the property of the record-owner. The investigating entity owns its determinations and the final record it produces.
- [0006] Prior art only partially protects the recipient or certifies that an effort was made to validate the owner's (supplier's or the organization's) identity. However, the aforementioned methods do not rigorously certify a record so that the recipient receives better information about the record attributes and the owner's identity, thus more thoroughly preventing misrepresentation and fraud.
- [0007] Moreover, the victim of fraud or the party accused thereof may be deficient in the ability to assert his rights, or defend such charges of fraud, by the absence of certified records with record attributes and/or more information, the parties identify to substantiate or refute such charges.
- [0008] There is significant potential for misrepresentation by the record-provider and a need for improvements to authenticate records rigorously.
- [0009] Some service-providers authenticate computer records or records captured by a computer, such as, emails and faxes, with digital date and time stamps. The records are maintained in read-only format so that their contents and attributes cannot be altered. The method does not authenticate record-attributes nor does it add the owner's (supplier's) identifying information to the record. One can change the date and time stamps by resetting the computer's internal clock and,

therefore, the method is unreliable. For greater reliability, the record is sent to a service-provider to attest its seal, date and time stamps and saved in a read-only format. The certified record is then sent to the owner and / or to third parties, at the owner's request. The service-provider maintains a copy, on its secure server, and can transmit it to a third party, later, at the owner's request.

- [0010] Alternatively, a service-provider licenses its software, which adds a digital seal, date and time stamps to a record stored on a computer. Date and time stamps, however, are not obtained from the computer's memory but accessed from a secure server. When a record is maintained only by the owner, its authentication is less reliable because a software hacker can alter the record or change the date and time stamp. A record is more reliable when it's maintained on a secure server (preferably, the server of the service-provider, but not necessarily).
- [0011] [The prior art does not express the need nor teach which record attributes and which identifying information, of the record-owner (including a supplier of product or service), the service-provider determines and appends to the original record. There is a need for a method to determine record attributes and add the owner's identifying information to the record before certifying it.]
- [0012] Some firms selling items on the Internet use another method of certification. For example, in 2003, "ebay" started requiring sellers of air, lodging, cruises and vacation packages to register with a seller-verification and dispute-resolution company. Before listing travel items, sellers must verify their firm's name, contact information and location with "SquareTrade", which permits registered sellers to display the "SquareTrade" seal next to their items listed for auction. Unfortunately, unregistered sellers can copy the seal and abuse it. ("ebay" does not permit individuals to sell vacation packages.)
- [0013] Thus, there is a need to examine items - such as, unused, transferable vacation packages – and determining if any restrictions apply and adding an item's attributes to its image before authenticating the entire record and posting the augmented record on the Internet. Items authenticated in the prescribed manner can be listed for sale on any website – not just on eBay. The augmented record has a record-number associated with it for locating and viewing the image of the item with the accompanying objective information, including date and time stamp, by accessing it from the service-provider's secure server.

- [0014] The prior art mostly relates to authenticating the identity of a person wanting access to secure data, a website, a secure server where he can perform or execute certain tasks, or to a physical location. Some of the art relates to digitally matching a person's biometrics with the information that is on the certifying authority's secure server. Other prior art requires an individual to provide password(s), key(s) and other confidential information – such as, the person's place and date of birth or mother's maiden name - before permitting access to a secure server or to a place. The art does not express a need to protect a third party from receiving misrepresented information.
- [0015] It is an object of this invention to reduce misrepresentation and conflict between the record-provider (including information about products and services offered by organizations) and recipients.
- [0016] It is a further object of this invention to provide information to protect recipients (saving them time and money and reducing their risks) so that they make decisions based on the most recent, accurate, reliable and complete information.
- [0017] It is also an object of this invention to protect record-owners by providing a method to authenticate their records so that they may assert their rights, after certification, in situations of conflict.
- [0018] Still a further object of this invention to remove the owner's (supplier's) bias from merchandise (object) attributes, occurrences at an event, or personal characteristics.
- [0019] It is an additional object of this invention to enhance trade and economic activity by improving the quality and the quantity of information that is available via the Internet or that is provided to recipients by other means.
- [0020] Another object of this invention is to provide multiple means for confirming the authenticity of records, which are sent to or accessible to third parties.
- [0021] Yet another object of the invention is to provide a means for sharing very personal information only with others willing to share and exchange the same information, wherein each party to the exchange is assured that the information they receive is genuine and not merely to secure their personal information.
- [0022] Still another object of the invention is to permit multiple parties to work independently or in cooperation to provide the entire service instead of it being supplied by a single service-provider. For example, party A determines the

objective attributes of the original record. Party A or B determines the identifying information of the record-owner (record-provider). Party A, B or C records the determinations into a form-like data structure. Party A, B, C or D maintains the entire record, including the determinations, on a secure server.

- [0023] It is an object of the invention that the method be used for authenticating records, documents and information about products and services provided by organizations and individuals.
- [0024] It is also an object of the invention to authenticate representations made by individuals about their personal characteristics, attributes, skills and qualifications and work related experience.
- [0025] It is also an object of the invention to authenticate an original record, which is an integrated production of one or more of sound, text, video, drawings and images of one or more of: an event, place, service, process, procedure, or object and the attributes include one or more of relevant descriptions and or measurements of: the event, place, service, process, procedure, or object, expressed by writing, drawing, displaying, and speaking or acting by the service-provider.

SUMMARY OF THE INVENTION

- [0026] The first and other objects of the invention are accomplished by utilizing a certifying authority to create, store, control and grant access to the first party's desired records or information in a digital format, making them selectively accessible to a third party. Such certifying authority in a first instance certifies the identity of the record-owner and validates his signature. The certifier also determines record attributes and the owner's identifying information and maintains the certified record, in read-only format, on a secure server. The record is either directly accessible to a third party (for example, via the Internet) or the service-provider can provide confirmation to a third party whether or not the record certified by it is authentic. Servers accessible via the Internet are vulnerable to malfunctions, to the service-provider's agents, to outside computer hackers and to virus attacks. Secure servers not accessible via the Internet are only vulnerable to malfunction and to the agents who are able to penetrate the security shield without authorization.
- [0027] In other aspects, deployment of the instant inventions involves one or more of the following steps in creating and using a secured record: (1) Determining and adding record attributes – such as, form, dimensions, specifications, expected use, and color - to the record, to the extent possible. (2) Adding the owner's (supplier's) identifying information; to the extent it is relevant. (3) Certifying the entire record, including the information determined added by the certifying authority, with a seal, a record-number, date and time, and location stamps. (4) Maintaining the entire record on a secure server. (5) Providing a means for a third party to access the entire record and be confident that it's authentic or providing a means for confirming whether the record received by a third party is authentic.
- [0028] Deployment of the instant invention protects and certifies to a recipient that the record is authentic by providing useful information about the record and its owner along with information about when and where the record was created and certified.
- [0029] Application of the invention avoids misrepresentation and conflict between the record-provider and recipients by inserting a service-provider between the two

- parties who adds objective information to the original record before certifying it. The certified record is more reliable, accurate and current.
- [0030] The receiving parties are protected, as well as save time and money, able to make decisions based on the most recent, accurate, reliable and complete information by using a service-provider who informs the public what sort of identifying information it tries to determine or seek from a record-owner (or from the supplier of information). For example, the certifier determines age, qualifications (degrees and institutions attended and organizations employed at), weight, height, race, hair and eye colors, skin complexion, baldness, name, signature and address when making determinations of a person. When determining the identifying information of a firm, the certifier seeks the business name, address, contact person, phone and fax numbers, email address, web address, where it's registered (incorporated), primary business function, the industry that it serves, and other relevant information. Over time, the list of attributes and identifiers can be enhanced or revised.
- [0031] Service-providers determine the attributes of a person, organization, pet, object, place, event, documents, art, process, etc. They document their determinations, which are verified against the record-owner's driver's license, passport, registration papers or by searching public databases, or by measuring the owner.
- [0032] People may choose not to provide personal information. In such a case, the service-provider records that the customer opted out. The recipient can then make his own inference about the record-provider's motives. If some information is not available, it is recorded as N/A.
- [0033] The objective of removing the owner's (supplier's) bias from the record attributes is accomplished, assuring objective information, by using a service-provider to make an unbiased determination. If the owner (supplier) does not agree with the determinations, he may seek a different service-provider.
- [0034] The object of providing multiple means for confirming the authenticity of records for third parties by having the service-provider issue a record-number at the end of the certifying process. It is used to locate the record on the server. At customer's request, a record-address where a third party can access, scrutinize and verify the record's authenticity is also provided. For example, an ad in a newspaper or on a website may have the URL (Universal Resource Locator)

address where an interested third party can view the authenticated record. The URL address can be typed into the address-field of a web-browser running on a computer to cause the entire augmented record to appear on the computer's monitor.

- [0035] The above and other objects, effects, features, and advantages of the present invention will become more apparent from the following description of the embodiments thereof.

NOVELTIES OF THE INVENTION

- [0036] It is an important aspect of the invention that the party determining the record attributes and the identifying information of the record-owner is different from the party owning and supplying the record and ultimately owning the entire record, including the certifier's determinations. Specifically, a record-owner requests a certifier to make determinations and append them to the original record and certify the entire record. The entire certified record is solely and entirely owned by the record-provider -- not by the certifier.
- [0037] The elements, which distinguish the invention from the prior art, follow. First, the certifier and the record-owner are distinct parties. Second, the certifier's determinations become part of the final certified record. Third, the entire record is maintained on a secure server, in read-only format.

DESCRIPTION OF THE INVENTION

- [0038] Examples of the invention are as follow. People post personal ads with their photos on matchmaking sites or in newspapers. Some provide pictures of pets for sale or to give away. Others provide pictures of items for sale. Some misrepresent information – such as, age, qualifications (degrees and institutions attended and organizations employed at), weight, and height - or provide an old photo. Alternatively, they exaggerate their own attributes or the attributes of the items for sale. Viewers do not know if the photo was brushed, if it is an old photo, or if the person's attributes or the identifying information are accurate. Some people pretend to be young and friends of children. They misguide the children in to a meeting or indulging in inappropriate behavior. If people were required to post certified information and photos on social websites, then exploiters would be deterred.
- [0039] Further, persons may be reluctant to post very personal information about themselves such as pictures, likes and dislikes, unless they are assured anonymity until a selected condition is met, which may include the willingness of another party to exchange the same information about themselves.
- [0040] Photos of people, pets, places and objects, recordings of events and processes, and documents are maintained on various recording media and / or servers. Some records, including video and sound recordings, are accessible via the Internet but are not well authenticated. The present invention describes a method for rigorously certifying records and maintaining them on secure servers, which can be made accessible to third parties.
- [0041] Alternatively, a copy of the certified record that the service-provider gives to the customer (or a replica of the copy) can be sent to a recipient. The recipient may then submit it to the service-provider to find out if the record he received matches the one that is on the service-provider's secure server. The record is located by using the record-number, which is part of the certified record. The original record is then digitally matched to the copy submitted in order to determine its authenticity.
- [0042] Alternatively, one or more certifying authorities can act as escrow agents for parties who wish to exchange information only upon assurance that they receive

a genuine record from the other party of the same information exchanged. When the parties agree to exchange information they provide the other party with a key or code unique to their records. Each party then provides the service provider holding the record(s) with the key to the other party's record and their own key. The service-provider only releases the information in the record to the requester when both parties have made the request. Thus making their own information available for release and the provider has validated that genuine authentic records exist for both parties.

- [0043] In any case, the records may be encrypted with a digital encryption key that the parties also exchange, but that the record holder does not possess. This eliminates the record holder, or a person having access to the record holder's system, from unauthorized viewing or release of the records. In creating such encrypted record the party has sole access to a secure private facility provided by the record holder, or their agent, and deploys or enters a password or other encryption key at the time they create the record in the secure facility, thus the key is known only to the record creator.
- [0044] In a preferred embodiment, a customer asks a licensed or a reputable service-provider to snap his photograph. The service-provider takes a digital photo, determines the customer's attributes – such as, age, qualifications (degrees and institutions attended and organizations employed at), gender, race, height, weight, hair and eye color, baldness, whether the person wears spectacles or uses hearing aid, whether the person has a speech impediment, and skin complexion – and appends the determinations and the customer's identifying information - such as, name and address – to the record and attests its seal with a record number, date, time and location stamp to the original record.
- [0045] In other embodiments, the certifying authority's seal is not used but instead the entire record (including the attributes and the record-provider's identifying information) is maintained on a secure server.
- [0046] In yet other embodiments, the customer is granted access to a secure facility for recording their own picture (s), with the service provider only identifying the person or things granted access to the secure facility. Specifically, the method comprises the following steps, which are executed by at one of the service-provider and the customer:

- [0047] A. Creating the original record.
- [0048] B. Converting it to digital format, if necessary.
- [0049] C. Determining the record attributes. For example, for people, the attributes are weight, race, height, gender, hair and eye color, and skin complexion. For products, the attributes are form, color, dimensions, expected use and benefits of the product, durability and other attributes.
- [0050] D. Determining the owner's identifying information. For a person, the identifying information is name, age and address. For an organization, offering a product or service, the identifying information is business name, address, contact person, phone and fax numbers, email address, web address, place of registration (incorporation), primary business function, the industry that it serves, and other relevant information.
- [0051] E. Recording the determinations (attributes and the identifying information) by appending them to the original record.
- [0052] F. Saving the entire record on a secure server in read-only format.
- [0053] G. Adding a record-number, date, time, and location stamps, service-provider's I.D. #, and the name of the person executing the method.
- [0054] H. Certifying the entire record by attesting it with the service-provider's seal.
- [0055] I. Maintaining the entire record on a secure server. And,
- [0056] J. providing a copy of the entire record to the customer on a recording medium that is preferred by the customer.
- [0057] If he customer requests that the record be maintained on a server that's accessible to third parties, via the Internet, the method further comprises an additional step, denoted K, providing a record-address (for example, a URL address) to access the record.
- [0058] The owner gives the record-address to a third party interested in accessing the record. Since the record is maintained on a secure server, when the third party accesses it he feels assured that the record is authentic. He benefits from the information appended to the record by the service-provider. The service-provider's seal is in the form of a digital certificate or other encrypted code or indicia that reliably verifies the provider and prevents the impersonation thereof.
- [0059] If the record is not accessible via the Internet, the recipient may submit the record to the service-provider to confirm its authenticity. The original certified

- record is located on the secure server, using the record-number, and it is verified whether the submitted copy is authentic by matching it to the one on the server.
- [0060] If the customer wants the record to be limited to a select few people, the method further comprises an additional step, denoted as L, in which the service-provider issues a password, or the customer creates the password so that it is not known by the service provider; the password being required for accessing the secure server and the authenticated record.
- [0061] An alternate embodiment authenticates a video recording created by the service-provider. The method comprises executing steps A) – J), or A) – K) if the recording is to be accessible via the Internet, or steps A) – L) if the access is to be restricted.
- [0062] An alternate embodiment authenticates a sound recording. Instead of viewing it, it is heard and instead of displaying it, it is played. In a more preferred embodiment, the method comprises executing steps A) – J), or A) – K) if the recording is to be accessible via the Internet, or steps A) – L) if the access is to be restricted.
- [0063] An alternate embodiment authenticates a photo or a video recording of a pet. The method comprises executing steps A) – J), or A) – K) if the recording is to be accessible via the Internet, or steps A) – L) if the access is to be restricted. In step C), the service-provider determines the attributes of the pet -- not of the record-owner. As a non-limiting example, the original record is optionally a photograph of a pet and the attributes in the more preferred embodiments include a combination of color, markings, hair length, plumage, gender, length, height and weight and the approximate age of the pet, and the like.
- [0064] Another alternate embodiment authenticates a document (for example, a drawing or a dissertation) that is in analog (printed) or digital format. The service-provider creates or examines the document and authenticates it. The method comprises executing steps A) – J), or A) – K) if the recording is to be accessible via the Internet, or steps A) – L) if the access is to be restricted. In step C), the service-provider records the document attributes – such as, file-size, file-name, title, abstract, keywords, table of contents, list of figures, charts and tables, subject and categories under which it is listed and its format. In step D), some

- identifying information about the owner is not relevant and so the service-provider types N/R for the attributes that pertain to the customer.
- [0065] Another embodiment authenticates a photo of an item that the customer wishes to sell. He brings the item to the service-provider and the method comprises executing steps A) – J) or B) – J) if the service-provider accepts the photo submitted by the customer. If the customer wants to post the photo on the Internet, the method comprises executing step K) and also step L) if access is to be restricted. In step C), the service-provider records as many attributes of the item, as deemed relevant and useful, by examining it. In step D), some of the identifying information about the customer is not relevant and so the service-provider types N/R in the database for the customer's personal attributes.
- [0066] For yet another embodiment, the customer requests the service-provider to witness and record (a) an event; (b) a place; (c) a process (or a procedure); or, (d) an object that can't be brought to the service-provider. The method comprises creating an integrated record, which may include photos, video and sound recordings, text and drawings; and, executing steps A) – J), or steps A) – K) if the integrated record is to be accessible via the Internet, or steps A) – L) if the access is to be restricted. Step C) comprises adding descriptions and measurements – such as, the mood, smell, texture, dimensions, and color - to the original record, expressed by writing, drawing, displaying, speaking or acting. The entire record is compiled in text, image, video and sound formats. For step D), some of the customer's identifying information is not relevant and so the service-provider types N/R in the record wherever applicable.
- [0067] Since a service-provider has fast transmission lines, large storage capacity on its servers and technical expertise, customers may request it to access records from a computer (possibly at a remote location). The method further comprises adding the record attributes – such as: whether it's an executable application and, if so, its intended use, a sound or video recording, a document, an image, alphanumeric data and, if so, its intended use; and adding other relevant information about the quality of the record and the record-size; address of where the record was accessed from; the date and time of access; attesting the service-provider's seal to the record; and maintaining the full record on a secure server

and on a portable recording medium for customer's use, as requested by the customer.

- [0068] Other embodiments of the invention applicable to using a dating service include methods wherein the service-provider authenticates a record of the person seeking to subscribe to a dating service by forming the original record using a template type form containing multiple fields, which the service-provider fills; the form fields corresponding to various attributes for example age, qualifications (degrees and institutions attended and organizations employed at), height, weight, gender, race, measurements of chest, waist and hip circumference, eye and hair color, facial hair, baldness, whether the person wears spectacles, or requires hearing aid, whether the person has speech impediment, skin complexion, and the like.
- [0069] In other embodiments the original record is a drawing, artwork or one or more photograph of an item, including a three dimensional digital representation of the item, and the like.
- [0070] In further embodiments the original record is an integrated production of at least one or more of sound, text, video, drawings and images depicting or capturing a place, event or process, including a procedure, and the attributes include one or more of relevant descriptions and measurements of the event, expressed by writing, drawing, displaying, speaking or acting by the service-provider.
- [0071] In yet other embodiments, the record may include any executable application to display images, sound and/or video recording; document; image; alphanumeric record and its most likely use; as well as characteristics describing the record size; where it was accessed; and, the date it was accessed.
- [0072] While the invention has been described in connection with a preferred embodiment, it is not intended to limit the scope of the invention to the particular form set forth, but on the contrary, it is intended to cover such alternatives, modifications, and equivalents as may be within the spirit and scope of the invention as defined by the appended claims.